

AMENDMENTS TO THE CLAIMS

Claims 1-35 and 38-61 were pending at the time of the Action.

Claims 3, 18, 28, 42, 51, and 59 are canceled.

Claims 1, 4-5, 12, 16, 19-20, 26, 29-30, 31, 38, 40, 43-44, 49, 52-53, 58, and 60-61 are amended.

Claims 1-2, 4-17, 19-27, 29-35, 38-41, 43-50, 52-58, and 60-61 remain pending.

1. (Currently Amended) A method comprising:

identifying a target service to which access is sought on behalf of a client;

causing a server operatively coupled to the client to request access to the target service on behalf of the client, from a trusted third-party, wherein the server provides the trusted third-party with a credential authenticating the server, information about the target service, and a service credential previously provided by the client to the server; and

requesting the trusted third-party to provide the server with a new service credential granted in the name of the client rather than the server such that the new service credential authorizes the server to access the target service on behalf of the client.

2. (Original) The method as recited in Claim 1, wherein the trusted third-party includes at least one service selected from a group of

1 services comprising a key distribution center (KDC) service, a certificate
2 granting authority service, and a domain controller service.

3
4 3. (Canceled).

5
6
7 4. (Currently Amended) The method as recited in Claim 1-Claim
8 3, wherein the new service credential is configured for use by the server and
9 the target service to which access is sought.

10
11 5. (Currently Amended) The method as recited in Claim 1-Claim
12 3, wherein the credential authenticating the server is a ticket that includes a
13 ticket granting ticket associated with the server.

14
15 6. (Original) The method as recited in Claim 1, further
16 comprising:

17 causing the trusted third-party to verify that the client has authorized
18 delegation.
19

20
21 7. (Original) The method as recited in Claim 6, wherein:
22 the trusted third-party includes a key distribution center (KDC); and
23
24
25

1 causing the trusted third-party to verify that the client has authorized
2 delegation includes verifying the status of a restriction placed on the ticket
3 originating from the client.
4

5 8. (Original) The method as recited in Claim 1, further
6 comprising:
7

8 causing the trusted-third-party to selectively determine if the client is
9 allowed to participate in delegation either based on information selected from a
10 group comprising an identity of the client, a group affiliation associated with
11 the client.
12

13 9. (Original) The method as recited in Claim 1, wherein the
14 server is a front-end server with respect to a back-end server that is coupled to
15 the front-end server, and wherein the back-end server is configured to provide
16 the target service to which access is sought.
17

18 10. (Original) The method as recited in Claim 1, wherein:
19 the trusted third-party includes a key distribution center (KDC);
20 the KDC provides a ticket-granting-ticket associated with the client to
21 the client; and
22 the client does not provide the ticket granting ticket to the server.
23
24
25

1 11. (Original) The method as recited in Claim 1, wherein:
2 the trusted third-party includes a key distribution center (KDC); and
3 the server requests the new credential in a ticket granting service request
4 message that includes a service ticket provided by the client to the server.
5

6
7 12. (Currently Amended) A method comprising:
8 identifying a target service to which access is sought on behalf of a
9 client; and

10 causing a server operatively coupled to the client to request access to the
11 target service on behalf of the client, from a trusted third party, wherein the
12 server provides the trusted third party with a service credential authenticating
13 the server, information about the target service, and a service credential
14 previously provided by the client for the service, and wherein the client ticket
15 includes implementation-specific identity information; and

16 requesting the trusted third-party to provide the server with a new
17 service credential granted in the name of the client rather than the server such
18 that the new service credential authorizes the server to access the service on
19 behalf of the client.
20
21
22
23
24
25

1 13. (Original) The method as recited in Claim 12, wherein the
2 implementation-specific identity information includes information selected
3 from a group comprising privilege attribute certificate (PAC) information,
4 security identifier information, Unix identifier information, Passport identifier
5 information, certificate information.

6
7 14. (Original) The method as recited in Claim 13, wherein the
8 PAC information includes compound identity information.

9
10
11 15. (Original) The method as recited in Claim 13, wherein the
12 PAC information includes access control restrictions for use as delegation
13 constraints.

14
15 16. (Currently Amended) A computer-readable medium having
16 computer-executable instructions for performing tasks comprising:

17 in a server, determining a target service to which access is sought on
18 behalf of a client coupled to the server;

19 requesting a new service credential from a trusted third-party by
20 providing the trusted third-party with a credential authenticating the server,
21 information about the target service, and a service credential associated with
22 the client and the requesting server such that issuance of the new service
23 credential authorizes the server to access the service on behalf of the client.
24
25

1 17. (Original) The computer-readable medium as recited in Claim
2 16, wherein the trusted third-party includes at least one service selected from a
3 group of services comprising a key distribution center (KDC) service, a
4 certificate granting authority service, and a domain controller service.

5
6 18. (Canceled).

7
8
9 19. (Currently Amended) The computer-readable medium as
10 recited in Claim 16 ~~Claim 18~~, wherein the service credential is configured for
11 use by the server and the target service.

12
13 20. (Currently Amended) The computer-readable medium as
14 recited in Claim 16 ~~Claim 18~~, wherein the credential authenticating the server
15 includes a ticket granting ticket associated with the server.

16
17
18 21. (Original) The computer-readable medium as recited in Claim
19 16, further comprising:

20 causing the trusted third-party to verify that the client has authorized
21 delegation.

1 22. (Original) The computer-readable medium as recited in Claim
2 21, wherein:

3 the trusted third-party includes a key distribution center (KDC); and

4 causing the trusted third-party to verify that the client has authorized
5 delegation includes verifying the status of a forwardable flag value as set by
6 the client.

7
8
9 23. (Original) The computer-readable medium as recited in Claim
10 16, wherein the server is a front-end server with respect to a back-end server
11 coupled to the front-end server, and wherein the back-end server is configured
12 to provide the target service.

13
14 24. (Original) The computer-readable medium as recited in Claim
15 16, wherein:

16 the trusted third-party includes a key distribution center (KDC);

17
18 the KDC provides a ticket-granting-ticket associated with the client to
19 the client; and

20 the client does not provide the ticket granting ticket to the server.

21
22 25. (Original) The computer-readable medium as recited in Claim
23 16, wherein:

24
25 the trusted third-party includes a key distribution center (KDC); and

1 the requesting server requests the new service credential in a ticket
2 granting service request message that includes a service ticket provided by the
3 client to the server.

4
5 26. (Currently Amended) A system comprising:

6 a credential granting mechanism configured to receive a request for a
7 new service credential from a server and in response generate the new service
8 credential granted in the name of a client rather than the server if delegation is
9 allowable, and wherein the request includes:

10 a credential authenticating the requesting server,

11 identifying information about a target service to which access is sought
12 on behalf of the a-client coupled to the server, and

13 a service credential that was previously granted to the client for use with
14 the server.
15

16
17 27. (Original) The system as recited in Claim 26, wherein the
18 credential granting mechanism is provided by a trusted third party and includes
19 at least one service selected from a group of services comprising a key
20 distribution center (KDC) service, a certificate granting authority service, and a
21 domain controller service.
22

23
24 28. (Canceled).
25

1 29. (Currently Amended) The system as recited in Claim 26-Claim
2 28, wherein the service credential is configured for use by the server and the
3 target service.

4 30. (Currently Amended) The system as recited in Claim 26-Claim
5 28, wherein the credential authenticating the server includes a ticket granting
6 ticket associated with the server, and which was previously granted by the
7 credential granting mechanism.

8
9 31. (Currently Amended) A system comprising:
10
11 a server configured to generate a request for a new service credential in
12 the name of a client rather than the server from a trusted third-party, the new
13 service credential being associated with a client and a target service, the
14 request comprising:

15 a credential authenticating the server,

16 information about the target service, and

17 a service credential associated with the client and the server.
18

19
20 32. (Original) The system as recited in Claim 31, wherein the
21 trusted third-party includes at least one service selected from a group of
22 services comprising a key distribution center (KDC) service, a certificate
23 granting authority service, and a domain controller service.
24
25

1 33. (Original) The system as recited in Claim 31, wherein the
2 credential authenticating the server includes a ticket granting ticket associated
3 with the server.

4 34. (Original) The system as recited in Claim 31, wherein the
5 server is a front-end server with respect to the service.

6
7
8 35. (Original) The system as recited in Claim 31, wherein the
9 server requests the new service credential in a ticket granting service request
10 message that includes the service ticket associated with the client and the
11 server.

12
13 36. (Withdrawn) A computer-readable medium having stored
14 thereon a data structure, comprising:

15 a credential authenticating a first server,

16 information identifying a second server, and

17 a service credential associated with a client and the first server.
18

19
20 37. (Withdrawn) The computer-readable medium as recited in Claim
21 36, wherein the credential authenticating the first server includes a ticket-
22 granting-ticket (TGT) and the service credential includes a service ticket.
23
24
25

1 38. (Currently Amended) A method comprising:
2
3 separately authenticating a server and a client;
4
5 providing the server with a server ticket granting ticket;
6
7 providing the client with a client ticket granting ticket and a service
8 ticket for use with the server;
9
10 providing the server with a new service ticket in an identity of the client
11 rather than an identity of the server for use by the server for use with a new
12 service without requiring the server to have access to the client ticket granting
13 ticket.

14 39. (Original) The method as recited in Claim 38, further
15 comprising:
16
17 causing the server to request the new service ticket on behalf of the
18 client by forwarding the server ticket granting ticket, information identifying
19 the new service, and the service ticket to a trusted third party.

20 40. (Currently Amended) A method comprising:
21 identifying a target service to which access is sought on behalf of a
22 client that has been authenticated using a first authentication method;
23 causing a server that is operatively coupled to the target service and the
24 client to request a service credential to itself from a second authentication
25

1 method trusted third-party by identifying the client and the first authentication
2 protocol; and

3 causing the server to request a new service credential in an identity of
4 the client rather than an identity of the server, for use by the server and the
5 target service, from the second authentication method trusted third-party,
6 wherein the server provides the trusted third-party with a credential
7 authenticating the server, information about the target service, and the service
8 credential to itself.

9
10
11 41. (Original) The method as recited in Claim 40, wherein the
12 second authentication method trusted third-party includes at least one service
13 selected from a group of services comprising a key distribution center (KDC)
14 service, a certificate granting authority service, and a domain controller
15 service.

16
17 42. (Canceled).

18
19
20 43. (Currently Amended) The method as recited in Claim 40-Claim
21 42, wherein the service credential is configured for use by the server and the
22 target service to which access is sought.

1 44. (Currently Amended) The method as recited in Claim 40-Claim
2 42, wherein the credential authenticating the server includes a ticket granting
3 ticket associated with the server.

4
5 45. (Original) The method as recited in Claim 40, further
6 comprising:

7 upon receiving a request for the new service credential from the server,
8 causing the second authentication method trusted third-party to verify that the
9 client has authorized delegation.
10

11
12 46. (Original) The method as recited in Claim 40, wherein the
13 server is a front-end server with respect to a back-end server that is coupled to
14 the front-end server, and wherein the back-end server is configured to provide
15 the target service.
16

17 47. (Original) The method as recited in Claim 40, wherein the
18 first authentication method is selected from a group of authentication methods
19 comprising Passport, SSL, NTLM, and Digest.
20

21
22 48. (Original) The method as recited in Claim 40, wherein the
23 second authentication method includes a Kerberos authentication protocol.
24
25

1 49. (Currently Amended) A computer-readable medium having
2 computer-executable instructions for performing tasks comprising:

3 identifying a target service to which access is sought on behalf of a
4 client that has been authenticated using a first authentication method;

5 causing a server that is operatively coupled to the target service and the
6 client to request a service ticket to itself from a second authentication method
7 trusted third-party by identifying the client and the first authentication
8 protocol; and

9 causing the server to request a new service ticket in an identity of the
10 client rather than an identity of the server, for use by the server and the
11 identified service, from the second authentication method trusted third-party,
12 wherein the server provides the trusted third-party with a ticket authenticating
13 the server, information about the target service, and the service ticket to itself.
14

15
16 50. (Original) The computer-readable medium as recited in Claim
17 49, wherein the second authentication method trusted third-party includes a
18 key distribution center (KDC).
19

20
21 51. (Canceled).
22

23 52. (Currently Amended) The computer-readable medium as
24 recited in Claim 49 ~~Claim 51~~, wherein the service ticket is configured for use
25 by the server and the target service.

1
2 53. (Currently Amended) The computer-readable medium as
3 recited in Claim 49 ~~Claim 51~~, wherein the ticket authenticating the server
4 includes a ticket granting ticket associated with the server.
5

6
7 54. (Original) The computer-readable medium as recited in Claim
8 49, further comprising:

9 upon receiving a request for the new service ticket from the server,
10 causing the second authentication method trusted third-party to verify that the
11 client has authorized delegation.
12

13 55. (Original) The computer-readable medium as recited in Claim
14 49, wherein the server is a front-end server with respect to a back-end server
15 that is coupled to the front-end server, and wherein the back-end server is
16 configured to provide the target service.
17

18
19 56. (Original) The computer-readable medium as recited in Claim
20 49, wherein the first authentication method is selected from a group of
21 authentication methods comprising Passport, SSL, NTLM, and Digest.
22
23
24
25

1 57. (Original) The computer-readable medium as recited in Claim
2 49, wherein the second authentication method includes a Kerberos
3 authentication protocol.

4
5 58. (Original) A system comprising:

6 a server configurable to:

7
8 identify a target service to which access is sought on behalf of a
9 client that has been authenticated using a first authentication method,

10 request a service credential to itself from a second authentication
11 method trusted third-party by identifying the client and the first
12 authentication method, and

13 subsequently request a new service credential, for use by the server
14 and the target service, from the second authentication method trusted third-
15 party,

16 wherein the server provides the second authentication method
17 trusted third-party with a credential authenticating the server, information
18 about the target service, and the service credential to itself in an identity of the
19 client rather than the server.
20

21
22 59. (Canceled).
23
24
25

1 60. (Currently Amended) The system as recited in Claim 58-Claim
2 59, wherein the new service credential is configured for use by the server and
3 the target service.

4
5 61. (Currently Amended) The system as recited in Claim 58-Claim
6 59, wherein the credential authenticating the server includes a ticket granting
7 ticket associated with the server.
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25